

KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

(11)Publication number: 1020020076750 A
 (43)Date of publication of application: 11.10.2002

(21)Application number: 1020010016853

(71)Applicant:

HAREXINFOTECH INC.

(22)Date of filing: 30.03.2001

(72)Inventor:

KIM, CHEOL GI

(51)Int. Cl G06F 17/60

(54) PAYING METHOD BY STORING FINANCIAL INFORMATION IN MOBILE COMMUNICATION TERMINAL AND SYSTEM THEREOF

(57) Abstract:

PURPOSE: A paying method by storing financial information in a mobile communication terminal and a system thereof are provided to enhance a security of a financial transaction by coding financial information of a client and storing the coded information in a mobile communication terminal using a managing number(password) of an electronic wallet designated by a user as a key of an encryption algorithm.



CONSTITUTION: A card applicant possesses a personal mobile communication terminal(10) having an optical transceiver as a mobile phone or a PDA. A financial institution(40) codes financial information including a card number, inputs the information in the mobile communication terminal(10), and issues a card. A POS terminal(20) receives the financial information from the mobile communication terminal(10) and performs a payment. A VAN company(30) receives an approval request of the POS terminal(20), transmits the request to a corresponding financial institution(40), and transmits the approval result to the POS terminal(20).

COPYRIGHT KIPO 2003

Legal Status

Date of final disposal of an application (20040628)

Patent registration number ()

Date of registration (00000000)

Number of opposition against the grant of a patent ()

Date of opposition against the grant of a patent (00000000)

Number of trial against decision to refuse ()

Date of requesting trial against decision to refuse ()

Date of extinction of right ()

(19) 대한민국특허청 (KR)
(12) 공개특허공보 (A)

(51) 。 Int. Cl. 7
G06F 17/60A2

(11) 공개번호 특2002 - 0076750
(43) 공개일자 2002년10월11일

(21) 출원번호 10 - 2001 - 0016853
(22) 출원일자 2001년03월30일

(71) 출원인 주식회사 하렉스인포텍
서울특별시 중구 필동2가 16 - 6
(72) 발명자 김철기
경기도성남시분당구야탑동 (탑마을) 경향아파트309 - 1502
(74) 대리인 조의제

심사청구 : 있음

(54) 이동통신단말기에 금융정보를 내장하여 결제하는 방법 및 그 시스템

요약

이동통신단말기에 금융결제정보를 내장하여 결제하는 방법 및 그 시스템은 광송수신기가 부착된 개인 휴대 이동통신단말기에 금융정보의 보안성을 증대시켜 내장하기 위한 것이다. 본 발명은 카드 발급 신청시 고객 고유의 전자지갑용 관리번호(비밀번호)를 암호키로 사용하여 카드번호와 유효기간등의 금융정보를 암호화하고, 이 암호화된 금융정보를 고객이 지정한 이동통신단말기에 직접 입력시키거나 통신망을 통해 입력시킨다. 또한, 본 발명은 금융정보가 내장된 이동통신단말기를 이용하여 결제시 본인의 전자지갑용 관리번호(비밀번호)를 입력하여 암호화된 금융정보와 그 관리번호(비밀번호)를 가맹점의 POS터미널(또는 카드조회기)로 광송신하고, 이를 수신하는 POS터미널(또는 카드조회기)에서 수신된 전자지갑용 관리번호(비밀번호)를 이용하여 그 관리번호(비밀번호)로 암호화된 금융정보를 복호화한다. 따라서, 본 발명은 고객의 전자지갑용 관리번호(비밀번호)가 유출되지 않는 한 암호화알고리즘을 알아도 고객의 금융정보를 사용할 수 없으므로, 기존 마그네틱이나 플라스틱 형태의 카드와 비교할 때 원천적으로 복제하여 사용할 수 없도록 하는 효과를 나타낸다. 또한, 개인의 금융정보를 한 곳에 모아 놓은 전자지갑의 역할을 함으로써 소비자의 편의성을 증가시키며 신용카드나 은행결제카드, 출입카드등 현재 카드가 적용되는 모든 분야에 채용할 수 있는 효과를 제공한다.

대표도
도 2

색인어
금융정보, 이동통신단말기, 카드번호, 비밀번호, 암호화, 보안

명세서

도면의 간단한 설명

도 1은 본 발명이 적용된 결제시스템을 나타내는 구성도.

도 2는 도 1 시스템에서 이동통신단말기에 금융결제정보를 내장하는 방법을 설명하기 위한 흐름도.

도 3은 금융결제정보가 내장된 이동통신단말기를 이용한 결제과정을 설명하기 위한 흐름도.

< 도면의 주요부분에 대한 부호의 설명 >

10 : 이동통신단말기 20 : POS터미널 (카드조회기)

30 : 뎀사 40 : 금융기관

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 광송수신기가 부착된 개인 휴대 이동통신단말기를 이용한 광결제시스템에 관한 것으로, 보다 상세하게는, 전자지갑용 관리번호(비밀번호)를 도입하여 그 이동통신단말기의 금융결제정보를 복제하여 사용할 수 없도록 하기 위한 이동통신단말기에 금융정보를 내장하여 결제하는 방법 및 그 시스템에 관한 것이다.

최근 결제수단으로 현금보다 사용 및 휴대가 간편한 카드(card)를 많이 이용하고 있다. 카드종류로는 신용카드(credit card), 현금카드, 직불카드, 교통카드와 같은 선불카드등 결제종류에 따라 다양하다. 현재 사용하고 있는 카드는 플라스틱이나 마그네틱(magnetic) 형태로, 자기기록면이 존재하여 거기에 카드 고유번호 및 유효기간 등 카드정보가 기록된다.

위와 같은 플라스틱이나 마그네틱형태의 카드에 대해, 분실 및 부당 사용될 우려가 있어 사용자가 항상 소지하고 있는 휴대폰이나 PDA등의 광송수신기가 부착되어 있는 개인 휴대 이동통신단말기를 카드 대용으로 사용하여 결제처리할 수 있도록 한 새로운 결제시스템이 동일출원인에 의해 선출원된 특허 제 2000 - 13426호의 "이동전화를 이용한 상거래시스템" 및 특허 제 2000 - 31640호의 "이동전화를 이용한 결제방법" 명세서에 기재되어 있다. 이 명세서들에는 널리 보급되어 있는 휴대용 이동전화에 광송신기를 부착하고, 신용조회단말기에 광수신기를 부착하여 신용카드 대신 이동전화와 신용조회단말기간의 광 송수신을 통해 거래를 수행할 수 있도록 하는 내용이 개시되어 있다.

발명이 이루고자 하는 기술적 과제

그런데, 위와 같이 현재 사용하고 있는 신용카드, 선불카드, 은행결제카드등 마그네틱형태의 카드 대용으로 이동통신단말기에 카드정보를 내장하여 사용할 때, 이동통신단말기 내부에 카드정보가 변형없이 내장되면 복제 사용 우려가 있다. 특히, 직접 이동통신단말기의 메모리에 카드정보를 입력시키는 경우 이동통신단말기 개발자가 전문적인 장비를 이용하여 이동통신단말기 메모리를 복제할 수 있는 우려가 있다. 그래서, 카드사나 은행등 카드발급기관은 현재 마그네틱카드에 내장된 정보와 동일한 형태로 이동통신단말기에 내장시키는 것을 피하려 하고 있다. 하지만, 불특정 다수가 사용하는 금융거래에서 개인별 비대칭키(PKI)를 이용하는 암호화시스템 등은 계산속도가 많이 걸리게 되므로 고객을 현재의 시스템보다 불편하게 만들게 된다. 또한, 대칭키를 사용하는 경우에는 수많은 POS터미널에 입력된 대칭키가 동일하

로 키 보호에 많은 어려움이 있게 된다.

따라서, 본 발명의 목적은 전술한 문제점을 해소하기 위하여 사용자가 지정한 전자지갑용 관리번호(비밀번호)를 암호화 알고리즘의 키로 사용하여 고객의 금융정보를 암호화하고 이를 이동통신단말기에 내장하여 금융거래의 보안성을 증가시킬 수 있도록 한 이동통신단말기에 금융결제정보를 내장하여 결제하는 방법 및 그 시스템을 제공함에 있다.

발명의 구성 및 작용

위와 같은 목적을 달성하기 위한 본 발명의 이동통신단말기에 금융결제정보를 내장하여 결제하는 방법은, 광송수신기가 부착된 개인 휴대 이동통신단말기를 카드 대신 사용하여 결제하기 위한 방법에 있어서, (1) 카드 발급 신청시 전자지갑용 관리번호(비밀번호)를 입력받는 단계와, (2) 상기 입력된 고객 고유의 전자지갑용 관리번호(비밀번호)를 이용하여 고객의 고유 카드번호를 포함하는 금융정보를 암호화하는 단계와, (3) 상기 암호화된 금융정보를 상기 이동통신단말기에 내장시키는 단계와, (4) 상기 이동통신단말기에 결제 비밀번호를 카드 신청시 입력한 전자지갑용 관리번호(비밀번호)로 일치시켜 놓는 단계와, (5) 거래행위시 상기 이동통신단말기에 전자지갑용 관리번호(비밀번호)를 입력하여 결제모드를 선택하는 단계와, (6) 결제모드에서 상기 이동통신단말기에 내장된 금융정보 및 전자지갑용 관리번호(비밀번호)를 광신호로 송신하는 단계와, (7) 상기 광신호의 금융정보와 전자지갑용 관리번호(비밀번호)를 수신하고, 수신된 전자지갑용 관리번호(비밀번호)를 이용하여 금융정보를 복호화하는 단계, 및 (8) 상기 복호화된 금융정보로 결제처리하는 단계를 포함한다.

또한, 본 발명의 목적을 달성하기 위한 이동통신단말기에 금융결제정보를 내장하여 결제하는 시스템은, 광송수신기가 부착된 개인 휴대 이동통신단말기를 카드 대신 사용하여 결제하기 위한 시스템에 있어서, 카드의 발급을 신청한 고객의 고유한 전자지갑용 관리번호(비밀번호)를 이용하여 고객의 금융정보를 암호화하고, 이 암호화된 금융정보를 고객이 지정한 이동통신단말기에 입력시키며, 결제요청한 금융정보에 대해 승인하는 금융기관과, 상기 금융기관으로부터 금융정보를 입력받아 내장하고, 결제모드에서 입력된 전자지갑용 관리번호(비밀번호)를 내장한 금융정보와 함께 광송신하는 이동통신단말기와, 상기 광송신되는 금융정보 및 전자지갑용 관리번호(비밀번호)를 수신하고, 수신된 전자지갑용 관리번호(비밀번호)를 이용하여 금융정보를 복호화하며, 복호화된 금융정보로부터 고객의 거래를 결제요청하는 POS터미널/카드조회기, 및 상기 POS터미널/카드조회기의 결제요청을 접수하여 상기 금융기관에 전달하고, 금융기관의 승인결과를 요청한 해당 POS터미널/카드조회기로 통보하는 뱅사를 포함한다.

이하, 첨부한 도면들을 참조하여 본 발명의 바람직한 실시예를 상세히 기술하기로 한다.

도 1은 본 발명이 적용된 결제시스템의 구성도를 나타낸다. 도 1에 나타난 결제시스템은 카드 신청인이 소유하고 있는 휴대폰이나 PDA등의 광송수신기가 부착된 개인 휴대 이동통신단말기(10)와, 카드번호를 포함하는 금융정보를 암호화하여 이동통신단말기(10)에 입력시켜 카드발급하는 카드사나 은행등의 금융기관(40)을 구비한다. 또한, 도 1의 시스템은 이동통신단말기(10)로부터 금융정보를 수신하여 결제처리하는 POS터미널(또는 카드조회기)(20)과, POS터미널(또는 카드조회기)(20)의 승인요청을 접수하여 해당 금융기관(40)에 전달하고 그 승인결과를 요청한 POS터미널(또는 카드조회기)(20)로 전달하는 뱅사(30)를 구비한다. 이러한 구성을 갖는 도 1 시스템의 이동통신단말기에 금융정보를 내장하여 결제처리하는 동작에 대해 도 2 및 도 3을 통해 설명한다.

먼저, 현재의 마그네틱 카드 대신 보안성을 증대시켜 이동통신단말기(10)에 카드발급하는 과정에 대해 설명한다.

고객은 본인 소유의 개인 휴대 이동통신단말기(10)의 카드 사용을 위한 서류를 작성하여 카드사나 은행 등 해당 금융

기관(40)에 신청한다. 이때, 단말기의 결제모드용 비밀번호를 추가로 기입한다(단계 201). 여기서, 결제모드용 비밀번호는 개인의 금융정보를 한곳에 모아 놓은 전자지갑용 관리번호이다. 전자지갑용 관리번호(비밀번호)는 통상 4자리이나 금융기관(40)의 필요에 따라 증가될 수 있다. 금융기관(40)은 신청서를 심사 후 승인이 나면 고객이 신청한 전자지갑용 관리번호(비밀번호)를 암호화 알고리즘의 키(key)로 사용하여 카드번호와 유효기간등의 금융정보를 암호화하여 고객이 지정한 이동통신단말기(10)에 입력한다(단계 202). 예를 들면, DES(Data Encryption Standard)와 같은 대칭키 암호화 기법의 알고리즘과 고객이 신청한 전자지갑용 관리번호(비밀번호)를 키로 사용해서 현재 마그네틱카드의 기록면에 기록될 카드번호와 유효기간 등의 평문정보와 금융기관 고유의 암호화된 정보를 다시한번 암호화한다. 즉, 본인의 암호를 모르면 풀수 없는 대칭키 형태의 알고리즘을 사용하여, 이동통신단말기(10)에 내장될 금융정보가 알려져도 키로 사용된 전자지갑용 관리번호(비밀번호)를 모르면 사용할 수 없다. 이로 인하여, 본인의 전자지갑용 관리번호(비밀번호) 유출이 없이는 암호화 알고리즘을 안다고 해도 사용이 불가능하게 되어 현재의 마그네틱 카드보다 보안성을 증가시키게 된다. 단계 202에서, 금융기관(40)은 금융정보의 일부분 암호화하거나 전화번호등의 기타 다른정보를 추가로 암호화할 수 있다. 예를 들면, 전화번호가 없는 PDA를 이동통신단말기(10)로 이용할 경우 PDA의 기기 고유번호를 추가로 암호화한다. 전화번호나 기기고유번호등의 기타 다른정보를 추가로 암호화할 경우, 결제처리시 그 정보를 본인 인증하는 데 사용할 수 있다. 금융기관(40)은 암호화된 금융정보를 이동통신단말기(10)에 케이블을 연결하여 직접 입력하거나 통신망을 이용하여 무선으로 송수신하여 입력한다. 즉, 고객이 이동통신단말기(10)를 소지하고 직접 방문한 경우 금융기관(40)은 안전을 위해 그 이동통신단말기(10)의 하단부에 마련된 인터페이스(미도시)를 통하여 암호화된 금융정보를 입력한다. 이동통신단말기(10)는 입력되는 금융정보를 내부 메모리에 저장하여 추후 카드 결제시 사용할 수 있도록 한다. 고객의 선택에 따라 통신망을 이용하여 이동통신단말기(10)에 정보를 입력할 수도 있다. 고객은 신용 승인 후 금융정보가 이동통신단말기(10)에 입력 완료되면 결제모드의 전자지갑용 관리번호(비밀번호)를 신청시 기입한 전자지갑용 관리번호(비밀번호)로 맞추어 놓는다(단계 203). 이때, 전자지갑용 관리번호(비밀번호)는 비가역 함수와 같은 형태로 암호화하여 이동통신단말기(10) 내부에 저장하는 방식을 택하면 보안성을 더욱 증가시킬 수 있다. 이러한 과정을 통해 이동통신단말기(10)를 마그네틱이나 플라스틱 형태의 카드 대용으로 사용할 수 있도록 발급한다.

도 2의 과정을 통해 발급된 금융정보를 내장한 이동통신단말기(10)를 사용하여 결제처리하는 과정에 대해 설명한다.

일반상점이나 전자상거래등에서 물품 대금 지불 또는 교통 요금 지불등을 해야 할 경우, 고객은 소지한 이동통신단말기(10)의 키패드 조작으로 전자지갑용 관리번호(비밀번호)를 입력하여 금융결제모드를 선택한다(단계 301). 결제모드의 전자지갑용 관리번호(비밀번호)는 카드 발급시 신청한 전자지갑용 관리번호(비밀번호)에 해당한다. 금융결제모드에서, 이동통신단말기(10)는 입력된 전자지갑용 관리번호(비밀번호)를 비가역함수로 암호화하여 그 값을, 비가역함수로 암호화하여 저장되어 있는 전자지갑용 관리번호(비밀번호)의 암호화 값과 일치하는 지를 확인한다(단계 302). 두 관리번호(비밀번호)가 일치한 것으로 확인되면, 이동통신단말기(10)는 정상적으로 결제모드를 동작시킨다. 단계 302에서 두 관리번호(비밀번호)가 일치하지 않으면 기설정 횟수 이상 관리번호(비밀번호)를 재입력하여 관리번호(비밀번호)를 확인한다. 만약, 관리번호(비밀번호)가 기설정 횟수 이상 일치하지 않으면(단계 304), 결제모드가 잠기도록 하여 전자지갑용 관리번호(비밀번호) 노출을 방지한다(단계 305). 정상적인 결제모드에서, 고객은 사용할 카드의 종류를 선택한 후(단계 303), 이동통신단말기(10)상의 기설정된 송신버튼을 누름에 의하여 이동통신단말기(10)에 내장된 금융정보 및 전자지갑용 관리번호(비밀번호)가 적외선의 형태로 송출된다(단계 306). 이때, 이동통신단말기(10)와 POS터미널(또는 카드조회기)(20)간의 통신은 자체적으로 암호화 알고리즘을 사용하여 보안을 증가시킨다. 이동통신단말기(10)는 신용카드정보, 직불카드정보, 선불카드정보등 카드종류별로 내장된 정보중 사용자에게 의해 선택된 카드에 대응하는 정보를 전자지갑용 관리번호(비밀번호)와 함께 광송신한다. 휴대폰이나 PDA, 노트북 등 휴대가능한 단말기에는 광송수신기가 부착되어 있어, 본 발명은 부착된 광송수신기를 이용하여 광송수신한다. 카드 가맹점의 POS터미널(또는 카드조회기)(20)은 광송수신기가 내외장 형태로 연결되어 고객의 이동통신단말기(10)로부터 광송신되는 금융정보와 전자지갑용 관리번호(비밀번호)를 수신한다. 통상, 이동통신단말기(10)와 POS터미널(또는 카드조회기)(20)의 광송수신기 사이의 거리는 대략 1m이내의 짧은 거리이고, 광을 사용하므로 직진성이 있어 금융정보 및 비밀번호가 녹취될 가능성이 없어 안전하다. 다만, POS터미널(또는 카드조회기)(20)의 소유자가 녹취하는 경우는 현재의 유선통신망을 녹취하는 것이 더욱 쉬우므로 그 경우를 논의하는 것은 무의미함을 쉽게 알 수 있다. POS터미널(또는 카드조회기)(20)은 별도의 암호화키를 보관할 필요없이 복호화알고리즘만 동작시키고, 수신된 전자지갑용 관리번호(비밀번호)를 이용하여 한번 더 암호화된 금융정보를 복호화한다(단계 307). POS터미널(또는 카드조회기)(20)은 복호화되어 원 상태로 복원된 금융정보를 기존의 금융거래시스템과 마찬가지로 뱅사(30)를 거쳐서 카드사(40)의 전산망에서 승인여부로

를 결정한다(단계 308). 만약, 수신되는 전자지갑용 관리번호(비밀번호)가 틀리면, 이 틀린 전자지갑용 관리번호(비밀번호)로 복호화된 금융정보 자체가 틀리므로 승인이 이루어지지 않게 된다. 한편, 이동통신단말기(10)에 금융기관(40)이 사용허락한 고객의 전화번호나 기기 고유번호 등 고객의 기타 다른정보가 전자지갑용 관리번호(비밀번호)를 이용하여 추가적으로 암호화되어 있을 경우, 이동통신단말기(10)는 암호화된 정보 송출시 전자지갑용 관리번호(비밀번호)와 현재 사용하는 전화번호나 기기 고유번호를 함께 송출한다. 이 경우, POS터미널(또는 카드조회기)(20)는 복호화된 정보내의 전화번호와 수신된 전화번호를 비교하여 본인 인증을 한다. 물론, 고객의 다른 정보를 이용하여 전화번호처럼 본인 인증할 수 있다. 따라서, 소액결제 또는 교통카드 등에서 금융기관(40)의 데이터베이스의 승인없이 빠른 시간에 POS터미널(또는 카드조회기)(20)에서 승인을 결정할 수 있게 되는 편리함을 가져온다.

이동통신단말기(10)의 전자지갑용 관리번호(비밀번호)를 기계적으로 알아내려면 전문가라고 하더라도 많은 시간이 걸리게 되며 그 시간동안 이동통신단말기(10)의 소유자가 분실신고를 할 수 있어 A/S신청 이외에는 이동통신단말기(10) 소유자의 동의없이 전자지갑용 관리번호(비밀번호)를 아는 것이 불가능하다. 또한, A/S를 신청할 때라도 전자지갑용 관리번호(비밀번호)를 변경한 후 A/S를 받기면 한번더 암호화된 고객의 금융정보를 풀 수 없게 된다. 그리고, 정상적인 결제모드에서 판매원등에게 결제를 위해 넘겨줄 경우에 1회만 결제되도록 하고 1회 결제 후에는 자동적으로 전화사용 모드로 변경되게 함으로써, 재사용시 다시 전자지갑용 관리번호(비밀번호)를 요구하도록 설계할 수도 있다. 이럴 경우, 식당이나 주유소등에서 거래의 안전을 위하여 고객이 항상 계산대로 가야만 하는 불편을 크게 개선할 수 있는 편리성을 주게 되므로, 이동통신단말기(10)를 통한 신용결제를 안심하고 사용하게 된다. 그리고, 이동통신단말기(10)의 결제모드에서 고객이 자신의 금융정보를 알고자 할 경우 카드정보확인메뉴를 선택하면 이동통신단말기(10)내의 복호화프로그램이 동작하여 화면에 카드번호와 유효기간등의 정보가 표시된다.

발명의 효과

상술한 바와 같이, 본 발명의 이동통신단말기에 금융결제정보를 내장하여 결제하는 방법 및 그 시스템은, 항상 소지하고 있는 광송수신기가 부착된 이동통신단말기에 고객마다 서로 상이한 대칭키로 금융정보를 암호화하여 입력하고, 이를 현재 마그네틱이나 플라스틱형태의 카드 대용으로 사용함으로써, 지갑을 별도로 소지할 필요 없이 이동통신단말기로 모든 결제를 할 수 있는 편리함이 있으며, 여러 카드와 각종 금융정보를 동시에 저장할 수 있는 전자지갑의 역할을 할 수 있다. 또한, 카드사에서는 기존 시스템을 변경하지 않고도 고객의 편의성을 증가시키고 보안성을 증대시켜 수익을 극대화할 수 있는 장점을 갖는다. 또한, 계속적으로 발급해야 하는 마그네틱이나 플라스틱 카드의 비용을 줄일 수 있고, 결제시 1회만 금융정보를 송신 가능케 하고 다시 전화모드로 원상복귀 하도록 설계하여 주유소나 음식점등 카드를 중업원에게 넘겨주는 경우에도 안전하게 금융거래를 이루게 할 수 있다. 그리고, 기존 인터넷 결제와 같이 브라우저상의 입력 필요에 의해 자신의 카드번호와 유효기간을 알아야 할 경우 카드정보확인메뉴에서 이동통신단말기 화면에 카드정보를 표시하도록 하여 기존 카드 결제에 그대로 적용할 수 있는 효과를 갖는다.

(57) 청구의 범위

청구항 1.

광송수신기가 부착된 개인 휴대 이동통신단말기를 카드 대신 사용하여 결제하기 위한 방법에 있어서,

- (1) 카드 발급 신청시 전자지갑용 관리번호(비밀번호)를 입력받는 단계;
- (2) 상기 입력된 고객 고유의 전자지갑용 관리번호(비밀번호)를 이용하여 고객의 고유 카드번호를 포함하는 금융정보를 암호화하는 단계;
- (3) 상기 암호화된 금융정보를 상기 이동통신단말기에 내장시키는 단계;
- (4) 상기 이동통신단말기에 결제 비밀번호를 카드 신청시 입력한 전자지갑용 관리번호(비밀번호)로 일치시켜 놓는 단계;

- (5) 거래행위시 상기 이동통신단말기에 전자지갑용 관리번호(비밀번호)를 입력하여 결제모드를 선택하는 단계;
- (6) 결제모드에서 상기 이동통신단말기에 내장된 금융정보 및 전자지갑용 관리번호(비밀번호)를 광신호로 송신하는 단계;
- (7) 상기 광신호의 금융정보와 전자지갑용 관리번호(비밀번호)를 수신하고, 수신된 전자지갑용 관리번호(비밀번호)를 이용하여 금융정보를 복호화하는 단계; 및
- (8) 상기 복호화된 금융정보로 결제처리하는 단계를 포함하는 방법.

청구항 2.

제 1항에 있어서, 상기 제 (2) 단계는 DES(Data Encryption Standard) 대칭키 암호화 기법의 알고리즘을 사용하며, 고객이 신청한 전자지갑용 관리번호(비밀번호)를 키로 사용해서 금융정보를 암호화하는 방법.

청구항 3.

제 1항에 있어서, 상기 제 (2) 단계는 금융정보의 일부만을 암호화하는 방법.

청구항 4.

제 1항에 있어서, 상기 제 (2) 단계는 상기 이동통신단말기에 할당된 전화번호를 포함하는 고객의 다른정보를 추가로 암호화하는 방법.

청구항 5.

제 1항에 있어서, 상기 제 (3) 단계는 상기 이동통신단말기에 금융정보를 직접 입력시켜 내장하는 방법.

청구항 6.

제 1항에 있어서, 상기 제 (3) 단계는 상기 이동통신단말기에 금융정보를 통신망을 통해 입력시켜 내장하는 방법.

청구항 7.

제 1항에 있어서, 상기 제 (5) 단계의 결제모드에서 상기 이동통신단말기의 금융정보 확인 메뉴를 선택하면 복호화프로그램이 동작하여 카드번호와 유효기간을 포함하는 금융정보를 이동통신단말기 화면에 표시하는 단계 (9)를 더 포함하는 방법.

청구항 8.

제 1항에 있어서, 상기 제 (5) 단계는

- (5a) 입력된 전자지갑용 관리번호(비밀번호)와 미리 일치시켜 놓은 결제 비밀번호가 맞는 지를 확인하는 단계;
- (5b) 상기 확인결과 맞지 않으면 기설정 횟수 이상 전자지갑용 관리번호(비밀번호)를 재입력받아 확인하고, 맞으면 카드종류를 선택하는 단계; 및
- (5c) 상기 기설정 횟수 이상 재입력되는 전자지갑용 관리번호(비밀번호)가 맞지 않으면 결제 모드를 잠금시켜 전자지갑용 관리번호(비밀번호) 노출을 방지하는 단계를 구비하는 방법.

청구항 9.

제 8항에 있어서, 상기 제 (6) 단계는 선택된 카드종류에 대응하는 카드번호를 포함하는 금융정보를 전자지갑용 관리번호(비밀번호)와 함께 송출하는 방법.

청구항 10.

제 4항에 있어서, 상기 제 (6) 단계는 암호화된 전화번호를 포함하는 고객의 다른정보를 금융정보, 전자지갑용 관리번호(비밀번호) 및 상기 이동통신단말기에 할당된 전화번호를 포함하는 고객의 다른정보와 함께 송출하며,

상기 제 (7) 단계는 수신된 전자지갑용 관리번호(비밀번호)를 이용하여 금융정보와 고객의 다른정보를 복호화하는 방법

청구항 11.

제 10항에 있어서, 상기 제 (8) 단계는 복호화된 고객의 다른정보와 수신된 정보를 비교하여 본인 인증하는 방법.

청구항 12.

제 11항에 있어서, 상기 제 (8) 단계는 복호화된 전화번호와 수신된 전화번호를 비교하여 본인 인증하는 방법.

청구항 13.

광송수신기가 부착된 개인 휴대 이동통신단말기를 카드 대신 사용하여 결제하기 위한 시스템에 있어서,

카드 발급 신청한 고객의 전자지갑용 관리번호(비밀번호)를 이용하여 고객의 금융정보를 암호화하고, 이 암호화된 금융정보를 고객이 지정한 이동통신단말기에 입력시키며, 결제요청한 금융정보에 대해 승인하는 금융기관;

상기 금융기관으로부터 암호화된 금융정보를 입력받아 내장하고, 결제모드에서 입력된 전자지갑용 관리번호(비밀번호)를 내장한 금융정보와 함께 광송신하는 이동통신단말기;

상기 광송신되는 금융정보 및 전자지갑용 관리번호(비밀번호)를 수신하고, 수신된 전자지갑용 관리번호(비밀번호)를 이용하여 금융정보를 복호화하며, 복호화된 금융정보로부터 고객의 거래를 결제요청하는 POS터미널/카드조회기; 및

상기 POS터미널/카드조회기의 결제요청을 접수하여 상기 금융기관에 전달하고, 금융기관의 승인결과를 요청한 해당 POS터미널/카드조회기로 통보하는 뱅스를 포함하는 결제시스템.

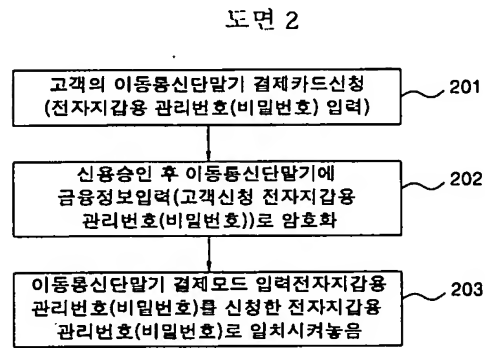
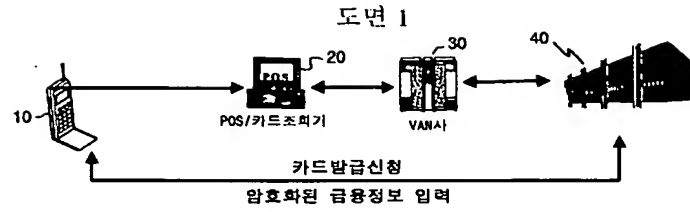
청구항 14.

제 13항에 있어서, 상기 이동통신단말기는 전화번호가 할당된 휴대폰 단말기이면 전화번호를 추가로 암호화하고, 전화번호가 없는 PDA 단말기이면 기기 고유번호를 추가로 암호화하며, 암호화된 전화번호 및 기기 고유번호를 금융정보, 전자지갑용 관리번호(비밀번호) 및 현재 사용하는 전화번호나 기기고유번호를 함께 송출하는 결제시스템.

청구항 15.

제 14항에 있어서, 상기 POS터미널/카드조회기는 수신된 전자지갑용 관리번호(비밀번호)를 이용하여 금융정보와 추가로 암호화된 전화번호나 기기고유번호를 복호화하고, 복호화된 전화번호나 기기고유번호를 수신된 전화번호나 기기고유번호와 비교하여 본인 인증하는 결제시스템.

도면



도면 3

